REMARKS/ARGUMENTS

This paper is submitted responsive to the Office Action mailed May 4, 2007. Reconsideration of the application in light of the accompanying remarks and amendments is respectfully requested.

In the action, the Examiner objected to the specification for failing to contain section headings. It is noted, however, that replacement pages for the specification were filed during the international stage of this application, and such replacement pages were transmitted to the national patent offices of interest. Those replacement page can be viewed on the WIPO web site, and they contain section headings as needed. It is believed that these documents are already of record in this application. If, however, they are not available to the Examiner and/or the USPTO, copies can and will be submitted by the undersigned.

The Examiner rejected claims 1, 2, 5-11, 14 and 15 as anticipated by US 5,657,388 to Weiss (Weiss '388). The Examiner also rejected claims 3, 4 and 16 as obvious based upon Weiss '388. Finally, the Examiner rejected claims 12, 13, 17 and 18 as obvious over a combination of Weiss '388 in view of US 6,981,141 to Mahne et al. (Hereafter Mahne).

Reconsideration of the rejections set forth above is respectfully requested. This is based upon a fundamental difference between the claimed invention and the teachings of Weiss '388. Weiss '388 does deal with "authentication", but this is only one of the four points raised in the present disclosure as a combination which must be addressed in order to effectively deal with security in a "faceless Environment".

By contrast, the present invention addresses all of these factors using multiple dynamically-changing-synchronized-codes to address each of the specific issues. According to the invention, one code is used for privacy, one for authentication, the time interval

between codes' change for integrity, and the unique set of changing codes for non-repudiation. Since various changing codes already exist, according to the invention, at two communicating ends independent of one another, no other momentary code other than that assigned for authentication needs to be exchanged. Once authenticated, the communication is secured with the momentary code other than that assigned for privacy on the premise that the receiving end should also have the decrypting codes because of authentication. In one simple stroke, according to the invention, authentication and privacy are effectively addressed with minimal complexity and computing overheads. This teaching is not at all obvious to a person skilled in the art considering the teachings of the art of record. This person would most likely attempt to address the specific issues of privacy with SSL or VPN, authentication with password and/or swipe or RFID cards, integrity with hashes and non-repudation with digital signatures and bio-metrics. In short, all these techniques would be needed according to the prior art, when the same objectives are accomplished according to the invention by using randomly changing codes.

It should be noted that although the Examiner has asserted that the personal code generation means taught in Weiss '388 has one or more encryption codes, the manner in which it obtains the encryption codes is fundamentally different from the present invention. Weiss '388 teaches that the token processor infers an encryption key. This involves sending the encryption key from the host processor to the token processor. The present invention features a personal code generation means capable of generating its own encryption codes, thus eliminating the step whereby an encryption code is inferred and therefore improving security.

The fact that the token processor of Weiss '388 is inferring an encryption key from the host processor means that the encryption code

is changing at the host to be sent to the token. The token processor is therefore not varying its encryption code independently of and in synchronization with the host processor because, by definition, these is no independent code being generated at the token end.

In summary, none of the cited prior art discloses or suggests a system in which the identification code of a code server and the encryption code of the code server change independently of and in synchronization with the identification code of the personal code generation means and the encryption code of the personal code generation means.

Based upon the foregoing, it is submitted that claims 1-18 define patentably over the art of record. An earnest and thorough effort has been made to address all issues and to place this application in condition for allowance. If, upon considering this paper, the Examiner believes that there are issues which remain that could be addressed by telephone interview, the Examiner is invited to telephone the undersigned to discuss and resolve same.

This paper is accompanied by authorization for a three month extension of time. It is believed that no other fee is due in connection with this paper. If any such fee is due, please charge same to Deposit Account 02-0184.

Respectfully submitted,

Azman Bin H J Zahari

By /george a. coury/
George A. Coury
Attorney for Applicant
Reg. No. 34,309
Tel: (203) 777-6628
Fax: (203) 865-0297

Date: November 5, 2007